Agile en plein essor : adopter les approches Agile et DevSecOps avec contrôle et conformité

Les principaux risques qu'une entreprise doit gérer quand son service des TI adopte Agile et DevSecOps.

pwc

À l'exception des jeunes startups qui sont authentiquement numériques et don nées « Agiles », la plupart des entreprises ont des structures complexes dotées de silos bien enracinés, de hiérarchies centralisées et d'une architecture technologique désuète établie depuis longtemps. C'est pourquoi l'adoption des approches Agile et DevSecOps doit être considérée comme une transformation technologique importante. D'autant que, à l'instar de toute transformation, elle comporte plusieurs risques qui doivent être soigneusement atténués.

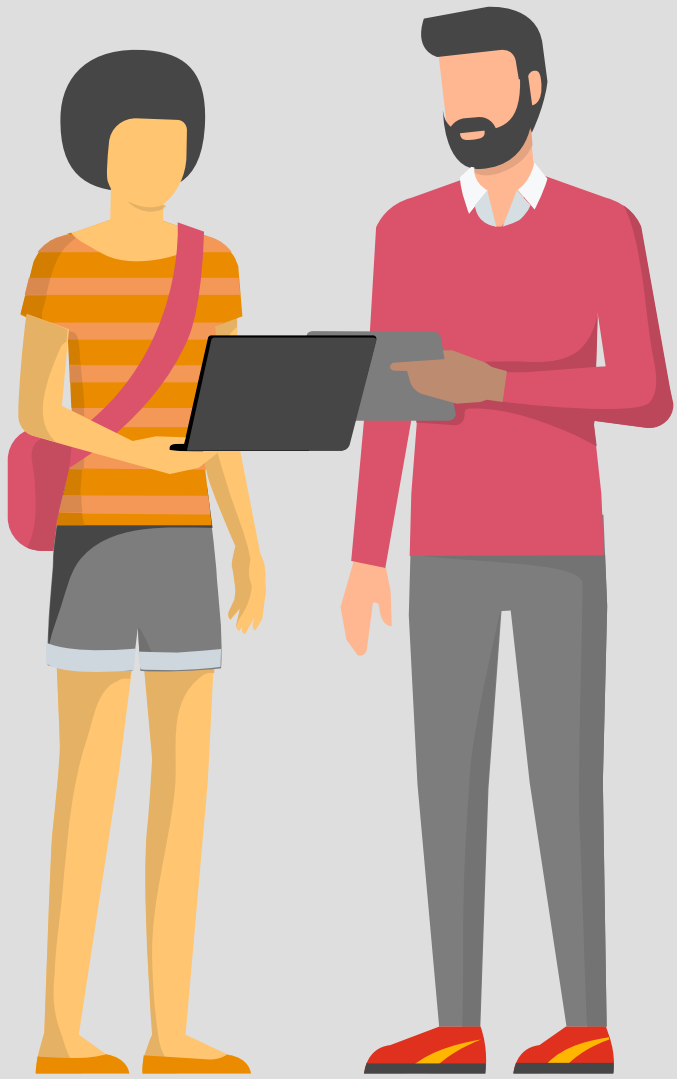
En général, nous constatons la présence de deux grands types de risque :

1. **Le risque d'adoption,** c'est-à-dire la capacité de l'entreprise d'adopter avec succès les approches Agile et DevSecOps.
2. **Le risque de gouvernance et de contrôle,** soit la capacité d'aligner la gouvernance, le risque et la conformité avec les approches Agile et DevSecOps, afin que la direction, les organismes de réglementation et les vérificateurs aient l'assurance que :
    a. les processus financiers, de planification et de surveillance demeurent valides;
    b. les contrôles internes sont maintenus tout au long du cycle de développement des systèmes (CDS);
    c. les produits mis en place dans le cadre du CDS sont conformes et adéquatement contrôlés.

Dans ce document, nous traitons d'une situation fréquente :

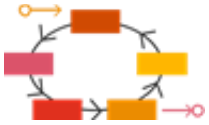
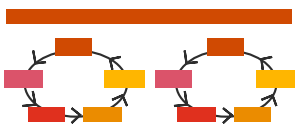
L'adoption enthousiaste des approches Agile et DevSecOps par l'équipe des TI, alors que ses risques et répercussions préoccupent les autres groupes de l'entreprise. Les lecteurs intéressés par une adoption plus globale de la méthode Agile (soit par toutes les fonctions de l'entreprise) sont invités à visiter cette page Web :

https://www.pwc.com/us/en/services/consulting/technology/taking-a-holistic-approach-to-enterprise-agility.html



Stades d'évolution

Les deux grands types de risque s'alignent aux stades évolutifs que les entreprises suivent souvent lorsqu'elles adoptent les méthodes Agile et DevSecOps. Car il n'existe pas qu'une seule voie vers la maturité, puisque le contexte de chaque entreprise est unique. Les principaux stades intérimaires sont décrits ci-après.

Stade	Caractéristiques	
Cascade	Processus de développement séquentiel dans lequel toutes les activités requises dans le cadre d'une phase doivent être terminées avant de passer à la suivante (par exemple, toute la conception doit être terminée avant le début de tout développement).	
Hybride	À ce stade, l'entreprise combine les structures en cascade et Agile. Le projet dans son ensemble suit des phases séquentielles définies (par exemple, la sélection du progiciel et l'analyse concordance-écart), avec certains développements itératifs au sein de chaque phase (comme la personnalisation).	
Projet pilote Agile	Les entreprises s'initient souvent à la méthode Agile dans le cadre d'un projet pilote. Elles ont ainsi un objectif précis et le réalisent en utilisant Agile, après quoi le projet prend fin. L'équipe affectée au projet doit suivre une formation initiale sur la méthode Agile et de nouveaux rôles doivent y être introduits (comme le chef de mêlée et le propriétaire de produit).	
Projets Agile	À ce stade, la méthode Agile est considérée comme une option endossée pour les efforts individuels. Un programme Agile a été développé, avec des formations officielles pour établir la répétabilité et la cohérence parmi les équipes.	
Équipe(s) de livraison continue	Ces équipes travaillent sur un aspect particulier et s'attardent à la demande la plus prioritaire comme « objectif », sans viser une conclusion définie. Elles doivent être structurées en fonction de la valeur qu'elles créent pour le client. Des outils DevSecOps/Agile appropriés devraient également être mis à profit pour la planification, la collaboration et l'automatisation.	
Agile à grande échelle	Alors que de plus en plus d'équipes adoptent la méthode Agile, toute l'entreprise doit évoluer dans cette direction (soit la gestion de portefeuille, les TI, les opérations, les finances, etc.). À ce stade, un cadre de travail commun et accepté est requis pour exploiter, synchroniser et gérer la coordination et les interdépendances des équipes impliquées dans de grandes initiatives.	

Points de friction :

comment adopter avec succès les approches Agile et DevSecOps?

La conversion à Agile et à DevSecOps, à travers des efforts individuels ou à l'échelle de l'entreprise, génère des impacts qui vont bien au-delà des TI et de leurs partenaires d'affaires. C'est pourquoi de nombreuses fonctions de l'entreprise devraient être intégrées dès les premiers stades de l'adoption.

La direction

- Les transformations à grande échelle exigent un appui solide de la part de la direction, dont les membres doivent favoriser l'inclusion et la responsabilité dans l'ensemble de l'entreprise pour assurer une adoption réussie.
- De nouvelles méthodes de gestion (comme le leadership serviteur) seront alors utiles pour permettre aux membres de la direction d'adopter la mentalité et les protocoles Agile de leurs équipes.

Les RH

- Dans un environnement Agile et DevSecOps, les effectifs de l'avenir exigent des compétences différentes (comme la conception créative et le développement piloté par les tests), de nouveaux rôles (par exemple, moins de gestionnaires de projet et plus de chefs de mêlée) et des façons de travailler transformées (comme passer d'une gestion « commandement et contrôle » à un « leadership serviteur »). Dans certains cas, l'emplacement des travailleurs et le recours à l'impartition, à la délocalisation et à l'automatisation peuvent être réexaminés. Cette transition de l'effectif exige un calibrage, une planification et une exécution réalisés avec prudence.
- Alors que les cadres de gestion du rendement sont habituellement centrés sur la performance individuelle, les entreprises Agile matures utiliseront plutôt un cadre de gestion qui favorise, encourage et récompense les succès de l'équipe.

La gouvernance de portefeuille et de projet

- Pendant la transition, plusieurs entreprises utiliseront à la fois les méthodes en cascade et Agile. Par conséquent, le processus de gestion de portefeuille et de gouvernance devra être mis à jour pour permettre la hiérarchisation, la sélection, le financement et le suivi des projets en fonction de plusieurs méthodologies.
- Les processus budgétaires annuels typiques ne prennent en charge que le financement par projet. Les processus devraient être améliorés pour permettre le financement dédié aux équipes permanentes.

L’approvisionnement

- Les contrats traditionnels fondés sur les produits livrables ne fonctionneront généralement pas pour des fournisseurs Agile en raison du niveau inhérent d’incertitude. Les contrats pour les fournisseurs et les outils DevSecOps devront comprendre une révision des ententes sur les niveaux de services et les autres mesures de succès.
- Les modèles de contrat standard comprennent généralement des modalités de paiement par étapes. Impliquer l’Approvisionnement dans les négociations contractuelles permettra d’atténuer les risques inhérents pour l’entreprise lors de l’adoption des approches Agile et DevSecOps.

Les risques et la conformité

- Il importe d’obtenir l’engagement des spécialistes et de la direction des groupes de gestion des risques, du contrôle des applications informatiques, de la conformité et de la réglementation afin qu’ils soient disponibles, bien informés et prêts à adopter de nouvelles façons de travailler. Il sera ainsi possible de favoriser leur participation en temps réel tout au long du cycle de vie du produit.
- Intégrer les groupes de la gestion des risques, du contrôle des applications informatiques, de la conformité et de la réglementation avant la phase de « conception » mène à une socialisation plus précoce entre les équipes, grâce aux diverses phases itératives.

Les contrôles généraux des TI

- Bien que les obligations et les objectifs en matière de contrôles demeurent inchangés, les contrôles doivent évoluer. Il importe d’impliquer les équipes d’audit internes et externes dans la modification des contrôles.
- Une hausse de l’automatisation à cet égard augmentera les risques liés aux outils d’automatisation. Ce faisant, les partenaires d’audit doivent savoir comment contrôler et tirer parti de l’automatisation.

Les fonctions d'audit

- Dans la foulée de l'adoption des approches Agile et DevSecOps, les vérificateurs seront confrontés à de nouveaux contrôles et propriétaires de produits, ainsi qu'à de nouvelles données en raison de la nature changeante du contexte en matière de risque. Ils devront donc adapter leur approche en conséquence.
- L'utilisation accrue d'outils d'automatisation devra se traduire par une évolution parallèle des centres d'intérêt de l'audit (pour y intégrer, par exemple, l'accès basé sur les rôles, les révisions d'accès et les tests automatisés).

Les finances et la fiscalité

- Les modèles existants en matière de décision et de suivi des dépenses en immobilisations par rapport aux dépenses d'exploitation reposent généralement sur l'approche en cascade, si bien qu'ils ne fonctionneront plus adéquatement.
- L'équipe de la fiscalité devrait être consultée afin de comprendre comment utiliser la R-D de façon optimale et de tirer profit des autres allégements fiscaux potentiels (par exemple, pour savoir si les prototypes et les maquettes peuvent être considérés comme de la R-D).

Les partenaires d'affaires

- Les propriétaires et les gestionnaires de produits sont essentiels dans un processus d'adoption des approches Agile et DevSecOps, car ils doivent être bien informés et disponibles, et ils doivent avoir du pouvoir. Les personnes qui comprennent les produits techniques, les processus d'affaires, les besoins des clients et les intervenants clés dans l'entreprise sont rares et généralement en forte demande. Les rendre disponibles pour des interactions quotidiennes avec les équipes Agile représente souvent un défi.
- L'objectif consiste à mettre en place un véritable partenariat, dans lequel l'équipe produit est considérée comme un tout, si bien que les silos entre les TI et les activités d'affaires n'existent plus.

Optimiser les chances de succès par des changements simultanés à la gouvernance, aux risques et à la conformité pendant le déploiement des approches Agile et DevSecOps

Compte tenu des nombreuses répercussions mentionnées dans les pages précédentes, les entreprises doivent apporter des changements aux processus, aux contrôles, aux outils, aux façons de penser et aux structures pour maintenir les fonctions de gouvernance, de risque et de conformité au même niveau. Chaque entreprise devra examiner attentivement ses progrès ainsi que son contexte unique (généralement par une analyse de l'impact du changement). Cela dit, les travaux habituels comprennent :

- La création d'un nouveau cadre de cycle de vie du produit (CVP) ou de CDS (avec les extrants et les approbations obligatoires) pour favoriser de respect de la conformité et des contrôles internes.
- La révision des matrices de risques et de contrôles, ainsi que les descriptions des contrôles sur le CDS. Habituellement, les contrôles généraux des TI (c.-à-d. la gestion du changement) peuvent demeurer les mêmes. Toutefois, les contrôles opérationnels et de surveillance peuvent nécessiter des mises à jour.
- La création ou la mise à niveau de programmes Agile et DevSecOps pour définir les protections requises afin d'assurer la cohérence et la répétabilité des processus à travers les équipes.
- La révision des outils utilisés dans le processus de développement et le pipeline DevSecOps, pour s'assurer qu'ils sont correctement « verrouillés », pour des raisons de fiabilité, et que l'ampleur des impacts possibles sur les contrôles est bien comprise.
- La révision des outils pour déterminer si les rapports SOC sont disponibles, puis comprendre quels contrôles sont couverts, la responsabilité et si les membres de l'équipe devraient obtenir des qualifications précises.
- La création de nouvelles procédures d'audit qui tiendront compte de la nature changeante des risques associés à l'utilisation de la méthode Agile.
- La mise en place de façons de travailler et de modèles d'interactions acceptés pour que les équipes de gestion des risques puissent fournir leur expert métier et leurs exigences sans perturber le travail des équipes Agile.
- La mise à jour des politiques et procédures sur les dépenses en immobilisations et les dépenses d'exploitation pour s'assurer que les projets Agile y sont traités et distingués correctement.

Modifier les activités de contrôle pour permettre l'essor de l'approche Agile

Alors que l'utilisation de l'approche Agile devient de plus en plus répandue, tous les responsables de la gestion des risques, de la conformité et de la certification doivent comprendre comment ces méthodes très puissantes peuvent coexister avec des contrôles efficaces. Grâce à une compréhension suffisante de l'environnement Agile et DevSecOps et des pratiques de pointe en matière de développement des contrôles, les professionnels du risque peuvent prendre les mesures adéquates pour intégrer des contrôles qui protégeront contre les risques et la non-conformité sans compromettre l'agilité requise.

Communiquez avec nous
Pour discuter plus en profondeur de l'intégration efficace des contrôles dans des environnements Agile, n'hésitez pas à communiquer avec nous.

Personnes-ressources

Andrew Schuster
(416) 687-8356
andrew.schuster@pwc.com

Sarah Shafey
(416) 687-8356
sarah.shafey@pwc.com

Karsten Kuhrmeier
(403) 509-7558
karsten.k.kuhrmeier@pwc.com

Ravinder Bains
(604) 806-7000
ravinder.bains@pwc.com

Merci!

© PwC, 2019. Tous droits réservés. PwC s'entend du cabinet américain membre, ou de l'une de ses filiales ou entités affiliées, et quelquefois du réseau mondial de PwC. Chaque société membre est une entité distincte sur le plan juridique. Pour obtenir de plus amples renseignements, visitez notre site Web à l'adresse : www.pwc.com/structure (en anglais seulement).